ConsumerReports.org

Don't get ripped off by credit card skimming at gas pumps

Cut your risk by learning what not to do when you fill up

Published: August 2013

Credit card skimmers hidden in gas pumps allow crooks to clone your credit or debit card.

Being able to pay by credit or debit card at the the gas station is a nice convenience. But when you swipe your card at the pump, you actually may be handing crooks what they need to steal money from your bank account at an ATM or go on a spending spree on your dime.

Credit card skimmers that thieves install where you swipe your card to pay at the pump can copy the account data from the magnetic stripe on the back of your card, along with your PIN if you type that in for a debit card transaction. In fact, what crooks prize most is capturing debit card data complete with PINs so they can make counterfeit cards to withdraw cash from your account at ATMs. “It’s an easy way to steal money with no guns or blood involved, and it’s also more lucrative than stealing credit card data to sell on the black market,” says Avivah Litan, a senior analyst at Gartner Research who specializes in fraud detection and prevention.

Just how lucrative? Two men indicted in July for a credit card skimming operation they set up at Murphy’s gas pumps in the parking lots of Walmart retail stores in Arkansas, Oklahoma, and Texas raked in $400,000 from April 2012 to January 2013, according to court documents filed in U.S. District Court for the Eastern District of Oklahoma.

The defendants, Kevin Konstantinov and Elvin Alisuretove, would leave skimmers in the gas pumps for one or two months, then retrieve them and wait another month or two before transferring the skimmed card information onto counterfeit cards they then used to withdraw cash from multiple ATMs, according to the court documents. On a single day in September 2012, for example, they used 75 counterfeit debit cards containing account data they’d obtained from gas pump skimmers to withdraw $45,280 from ATMs in the Oklahoma City area, the indictment states.

Criminals running skimming operations have been improving the technology they use to make stealing card data even easier, so card issuers and gas station owners need to step up their game to fight back, security experts say. Many different gas pumps can be opened with the same master keys, so crooks need only get copies of a limited set of master keys to get into pumps to install skimmers. Increasingly, they are using wireless internal skimmers that transmit the card data to them via Bluetooth devices, so they don’t even have to take the risk of retrieving the skimmer from the pump to download stolen card data.

“They just need to be within 30 feet of the skimmer, so one guy can go in to buy a Slurpee and distract the clerk while his partner sits in their car near the pumps downloading all of the stolen card data,” said Al Pascual, senior analyst of security risk and fraud at Javelin Strategy & Research.

Some gas stations are beginning to upgrade to pumps that have payment terminals equipped with antitampering devices, but that change is only occurring gradually because upgrades can cost $4,000 to $12,000 per pump, according to Litan.

How to minimize risks posed by debit and credit card skimmers

- To totally avoid becoming a skimming victim at the pump, use cash when you buy gas, which also should knock down the price per gallon you’ll pay.
- Use a credit card rather than a debit card at the gas pump, and preferably one that provides an attractive cash-back rate for gas. It's rare to see a lower price at the pump for debit-card transactions compared with credit-card transactions, according to Jeff Lenard, spokesman for the National Association of Convenience Stores. While some stations offer discounts both for cash payments and PIN-based debit transactions, Lenard said in most cases, discounts apply only when you pay with a specific convenience store’s debit cards tied to a loyalty program, such as those offered by the Savannah, Georgia-based Parker’s chain.
- If you must use a debit card, never type in your PIN. Instead, select the option on the screen that allows you to have your debit card purchase processed as a credit card transaction. The purchase still is debited from your checking account, but you won’t need to enter your PIN, which is what the bad guys need to withdraw cash from your account at an ATM.
- Monitor your bank and credit card accounts regularly to spot unauthorized charges or cash withdrawals and report them immediately. Under federal law, delays in reporting fraudulent transactions can increase your liability for losses. For more details on your legal liability for fraud-related losses on credit and debit cards, see this helpful advice from the Federal Trade Commission.

—Andrea Rock